CLAIMS

1. Apparatus for consolidating key updates provided in records that each comprise an encrypted key corresponding to a node of a key hierarchy and encrypted using a key which is a descendant of that node, hierarchy-node information for both the encrypted and encrypting keys, and key-version information for at least the encrypted key; the apparatus comprising a communications interface for receiving said records, and a manager for maintaining, on the basis of the received records, a key tree with nodes corresponding to nodes in said hierarchy, the manager being arranged to store in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded.

2. Apparatus according to claim 1, wherein the manager is arranged to store each said most up-to-date version of a said encrypted key by storing the record containing the latter with any previously-stored record that is thereby superseded being discarded.

3. Apparatus according to claim 1, wherein the manager is arranged to store in association with each tree node, along with the most up-to-date version of the corresponding encrypted key stored for each encrypting key used in respect of that encrypted key, version information for the encrypting key used to encrypt said most up-to-date version of the encrypted key, this version information being included in the record providing said most up-to-date version of the encrypted key.

4. Apparatus according to claim 3, wherein the manager is arranged to replace the version of the encrypted key stored in association with a tree node for a particular encrypting key, with any subsequently received later version of that key provided the latter has been encrypted with a version of the encrypting key that is the same or later than the version used for encrypting the existing stored encrypted key.

5. Apparatus according to claim 1, further comprising a working-set generator for processing the key tree to generate a subset of the tree enabling, at least within a target failure rate, all clients associated with the key hierarchy to recover the current root key of the latter.

6. Apparatus according to claim 5, wherein the working set generator comprises control means for receiving feedback on the current root-key recovery failure rate and for controlling the size of said subset to approach the actual failure rate to said target failure rate.

7. Apparatus according to claim 6, wherein the working set generator further comprises means for determining the likelihood of a tree node being required to enable recovery the current root key, these means being based on at least one of the age of the node, or of an encrypted key associated with it, and an estimate of the number of possible clients that will need the node.

8. Apparatus according to claim 1, wherein the manager is arranged to maintain said tree only in respect of keys corresponding to the nodes of a predetermined sub-hierarchy of said hierarchy and keys for the path from the head of this sub-hierarchy that terminates at the root of the hierarchy.

9. A system comprising apparatus according to claim 1, and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal of members to a group, the key-hierarchy manager being arranged to output said records both to currently available members of said group and to said apparatus as notification of the changes made by the key-hierarchy manager to the key hierarchy, said apparatus being arranged to provide said key tree, or a subset of it, to members of said group who subsequently become available as a consolidated notification of the changes made by the key-hierarchy manager to the key hierarchy whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin.

10. A system comprising apparatus according to claim 1, and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal of members to a group, the key-hierarchy manager being arranged to output said records to said apparatus, said apparatus being arranged to provide said key tree, or a subset of it, to members of said group as a consolidated notification of the changes made by the key-hierarchy manager to the key hierarchy whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin.

11. A system according to claim 10, wherein the key-hierarchy manager and said apparatus form part of an anonymous group content distribution arrangement; the key tree, or a subset of it, being sent to group members in association with content encrypted with a key that is one of:

- the key-hierarchy root key, and
- a key encrypted using the key-hierarchy root key and provided in encrypted form along with the encrypted content.

12. A system comprising multiple apparatuses according to claim 1, and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal of members to a group and for outputting key update records reflecting changes made to the key hierarchy; the apparatuses being configured in a multiple-level hierarchical arrangement comprising a first-level apparatus arranged to receive the records output by the key-hierarchy manager, and one or more lower levels of apparatuses each arranged to receive the key tree, or a subset of it, produced by a said apparatus at the next level up, the apparatuses at the lowest level of the hierarchical arrangement each being arranged to provide its key tree, or a subset of it, to a respective sub-group of members of said group; the apparatuses at each level of said hierarchical arrangement, other than said first level, each being arranged to maintain its said tree only in respect of keys corresponding to the nodes of a respective predetermined sub-hierarchy of said key hierarchy and keys for the path from the head of this sub-hierarchy that terminates at the root of the key hierarchy.

13. A method of consolidating key updates provided in records each comprising an encrypted key corresponding to a node of a key hierarchy and encrypted using a key which

is a descendant of that node, hierarchy-node information for both the encrypted and encrypting keys, and key-version information for at least the encrypted key; the method comprising a step of maintaining, on the basis of said records, a key tree with nodes corresponding to nodes in said hierarchy, this tree-maintenance step comprising a sub-step of storing in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded.

14. A method according to claim 13, wherein in said sub-step each said most up-to-date version of a said encrypted key is stored by storing the record containing the latter with any previously-stored record that is thereby superseded being discarded.

15. A method according to claim 13, wherein in said sub-step the version information of the encrypting key used to encrypt said most up-to-date version of the encrypted key is stored with the latter.

16. A method according to claim 13, wherein in said sub-step the version of the encrypted key stored in association with a tree node for a particular encrypting key, is replaced with any subsequently received later version of that key provided the latter has been encrypted with a version of the encrypting key that is the same or later than the version used for encrypting the existing stored encrypted key.

17. A method according to claim 13, further comprising the further step of processing the key tree to generate a subset of the tree enabling, at least within a target failure rate, all clients associated with the key hierarchy to recover the current root key of the hierarchy.

18. A method according to claim 17, wherein the further step comprises receiving feedback on the current root-key recovery failure rate and controlling the size of said subset to approach the actual failure rate to said target failure rate.

19. A method according to claim 18, wherein said further step further comprises determining the likelihood of a tree node being required to enable recovery the current root

key, this determination being based on at least one of the age of the node, or of an encrypted key associated with it, and an estimate of the number of possible clients that will need the node.

20. A method according to claim 13, wherein said tree is maintained only in respect of keys corresponding to the nodes of a predetermined sub-hierarchy of said key hierarchy and keys for the path from the head of this sub-hierarchy that terminates at the root of the hierarchy.

21. A method of providing key updates to members of a group, comprising the steps of:

- managing a key hierarchy in dependence on the addition and/or removal of members to said group and outputting, as notification of the changes made to the key hierarchy, records that each comprise an encrypted key corresponding to a node of the key hierarchy and encrypted using a key which is a descendant of that node, and hierarchy-node and key-version information for both the encrypted and encrypting keys; and
- consolidating said records according to the method of claim 13 and providing said key tree, or a subset of it, to members of said group whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin.